What Is a VPN? Definition, How It Works, and More

Written by Luis Millares, techrepublic.com, Published November 6, 2024

A VPN (virtual private network) encrypts your internet traffic and protects your online privacy. Find out how it works and why you should use it.

VPNs encrypt your online traffic and allow you to change your IP address, making it appear as if you're in a different location used in the following ways:

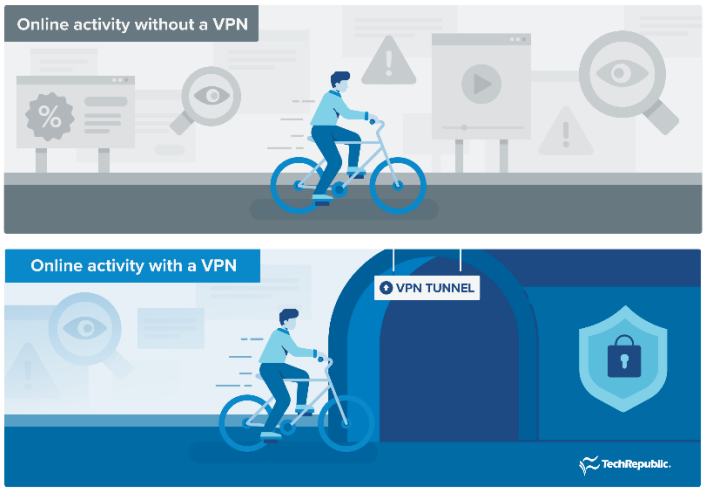
- To access region-locked content online such as shows or movies on streaming services
- To provide remote workers secure access to company resources
- To add an extra layer of anonymity and privacy while browsing online

Read our in-depth guide below to learn more.

A VPN, or a virtual private network, is a mechanism used to establish a secure connection between a device and a network, such as a remote employee's computer and a company's internal server. Organizations use VPNs to secure these connections and prevent potential threats from accessing and taking advantage of sensitive information.

In this article, we define what a VPN is, how it works, and how it can benefit you and your organization.

What is a VPN?



Online activity without vs. with a VPN. Image: TechRepublic

A VPN encrypts and hides online activity and sensitive information, such as browsing history and IP addresses, to keep your connection secure.

Think of online activity on unsecured public Wi-Fi as riding a bike on an open road; bikers and everything they're doing are visible — what sites they've visited, where they're coming from, and at what times they traveled. Online activity secured through a VPN represents a private tunnel for bikers to travel through with their activity and information hidden.

Whether you're an individual or a business, using a VPN can help protect your online data from potential threats.

How do VPNs work?

When you want to visit a website using a secure connection, you must first connect to the VPN using the app orbrowser extension.

The VPN generates a private connection that encrypts your internet activity and makes it unreadable. Once encrypted, the internet data is routed to a VPN server that masks your IP address, adding a layer of anonymity to your connection.

Finally, the VPN decrypts the data and sends it to the site you're visiting, creating the illusion to possible threat actors that your machine connected from the VPN server's location instead of your actual whereabouts.

This process makes sure that any data or information that can be tied back to you is scrambled and untraceable before it reaches your internet service provider.

Types of VPNs

There are quite a few types of VPNs, but three of the most common are remote access, site-to-site and personal VPNs.

- **Remote-access VPNs** allow users to connect to a remote network securely. Companies typically use this type of VPN to allow remote employees to safely access resources through a secure corporate network. Enterprise VPNs such as Perimeter 81 and NordLayer fall under this category.
- **Site-to-site VPNs** are used by large organizations to connect multiple networks to enable secure communication and resource sharing across different business headquarters. These networks, known as intranets, are common in big corporations with multiple locations, vast resources, and numerous data sources.
- **Personal VPNs** are designed for individual users, offering access to a VPN provider's servers to protect personal information and unblock georestricted content. Examples of personal VPNs are NordVPN, Surfshark, and ExpressVPN.

VPN benefits vs. VPN drawbacks

Depending on the service provider, VPNs can come with a range of potential benefits and limitations.

Benefits of VPNs	Drawbacks of VPNs
Secures data and internet traffic	Slower internet speed
Prevents tracking and allows for anonymity	Quality VPNs aren't free
Access to georestricted content	Not all VPNs are secure

Benefits of VPNs

Let's delve into three significant benefits of VPNs and how they can enhance online security and privacy.

Secures your data and internet traffic

A VPN's ability to protect user data through encryption is one of its most important benefits. As many workforces heavily rely on the internet, secure access to corporate resources has become a necessity. As more companies adopt hybrid and remote working environments, VPN protection has become increasingly vital.
Through VPNs, sensitive information such as browsing activity, IP addresses, and private communications within businesses and organizations can be protected — whether you're in a remote workplace or not.

Prevents tracking and allows for anonymity

VPNs prevent tracking and allow for greater anonymity as marketing websites and malicious actors would have a harder time tracking down a device's specific IP address.
There are even VPNs that route and encrypt user traffic to two or more servers through a process called multihop — adding an even higher level of privacy.

Enables access to georestricted content

Because a VPN server allows you to use an alternate IP address and location, you can make it appear to unauthorized observers that you're using the internet from a location of your choosing to access geographically restricted content.
This can be handy if you're traveling in another country and need to access a site or an online resource that's only available in a certain location. For example, if you set your location to a VPN server in Switzerland, all the websites you visit will perceive you as someone using the internet from that country.

Drawbacks of VPNs

While VPNs can offer numerous benefits, it's important to consider the potential drawbacks.

Quality VPNs aren't free

While there are free VPNs available, you will benefit the most from a paid solution. Quality VPNs come at a price because of the need for providers to obtain the right server hardware, to locate servers in multiple countries, and ensure these servers operate securely.
Paid VPNs also include more robust security protocols that protect user data and typically provide unlimited bandwidth for your internet activity.
Fortunately, VPN providers typically offer a range of subscription plans to accommodate diverse needs and budgets.

Slower internet speed

Another drawback of VPNs is the slower than usual internet connection. Because you're routing your internet traffic through multiple steps, there's an inevitable slowdown in real-world speed.
Slower speeds can also be the result of busy VPN servers, as a server theoretically handles thousands of connections from all over the world.

Not all VPNs are secure

It's important to understand that while most VPNs are effective security solutions, not all VPN providers offer the same level of protection. Some VPNs have had a history of reportedly logging and selling user data. This is why looking into a VPN's no-logs policy and third-party security testing are important steps before integrating a VPN into your organization.

Factors that affect VPN pricing

As most VPNs require a paid subscription, here are some factors that determine their cost.

Security and encryption

As a security product first and foremost, a VPN's cost is affected by the level of security it provides to the end-user. Proven security tunneling protocols such as OpenVPN, WireGuard, and IKEv2 are usually offered in more expensive VPN services. Having military-grade AES-256 encryption is another important tenet of VPNs that influences the eventual cost.

Server network

Generally, the more servers a VPN has the more expensive it is to run. This is because having servers in multiple locations around the world costs money to maintain.
The quality of these servers also affect pricing, as access to more secure and faster servers can be more expensive.

Features

Extra features can affect VPN pricing. Aside from providing an encrypted connection, some VPNs will include specialized features such as data breach monitors and ad blockers.
VPN providers can also offer their VPN on multiple platforms such as Windows, macOS, Android, iOS, browsers and smart TVs — all of which cost money on the side of the VPN provider.

Plan duration and length

Plan duration and length will also determine the final VPN cost. As a baseline, almost all VPN providers offer at least a one-month subscription, ranging from as low as $8 to as much as $20 per user, per month.
To lessen the cost, most VPNs offer longer plans that range from one to three years, often at a reduced monthly rate.

VPN security

Outside of encryption, there are other aspects of VPNs that impact overall security.

- **No-logs policy:** A no-logs policy is a VPN provider's assurance to customers that it doesn't log or keep track of any user data.
- **Independent security audit:** VPNs can bolster their security claims through independent security audits. These third-party tests can show prospective users that a VPN's security promises, such as a no-logs policy, are legitimate and backed by evidence and data.
- **Five Eyes Alliance (FVEY):** The Five Eyes alliance is an intelligence-sharing alliance comprising the United States, the United Kingdom, Australia, New Zealand and Canada. These countries have a history of surveillance on citizens, thus, VPNs that operate from these states can pose security risks. VPNs based in an FVEY country can still provide quality security but it's a valid reason to try other options that operate in more privacy-friendly nations.

When evaluating your options, make sure you understand which of these security features or others are available to you.

Popular VPN providers

Some of the best VPN providers today are NordVPN, ExpressVPN, and CyberGhost VPN.

NordVPN

If you're a privacy enthusiast, I highly recommend NordVPN. NordVPN offers built-in protection against malware, ads, and trackers through its Threat Protection Pro feature. NordVPNhas a unique encrypted file-sharing system that's ideal for users who regularly share sensitive files or documents. It also has specialized security servers such as obfuscated servers, double VPN servers, and P2P servers for additional security.

To learn more, check our full NordVPN review.

ExpressVPN

If having a user-friendly VPN app is your priority, I suggest going for ExpressVPN. ExpressVPN's easy-to-use and well-designed application accommodates both less tech-savvy and more advanced users. This is shown in both its desktop app and browser extension. On top of that, ExpressVPN provides consistent speeds and fast performance with its server fleet spanning 105 countries.

To learn more, read our full ExpressVPN review.

CyberGhost VPN

For those that want specialized servers, CyberGhost VPN is my recommendation. Out of the box, it categorizes its VPN servers into those optimized for streaming, gaming, and torrenting. This means you won't have to worry about looking for which servers are best for your specific use case. Right now, CyberGhost offers an extensive collection of servers across 100 countries and 126 locations.

To learn more, read our full CyberGhost VPN review.

If you're on the fence about paying for a VPN subscription but are still interested in how VPNs can work for you, our team has got you covered. I highly recommend checking out TechRepublic's video feature on the best free VPNs to try.